On Ranks of Twists of Elliptic Curves and Power-Free Values of Binary Forms

Stewart, C.L.; Top, J.

Published in:
Journal of the american mathematical society

Publication date:
1995

JOURNAL OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 8, Number 4, October 1995

ON RANKS OF TWISTS OF ELLIPTIC CURVES AND POWER-FREE VALUES OF BINARY FORMS

C. L. STEWART AND J. TOP

Dedicated to Professor Wolfgang Schmidt on the occasion of his sixtieth birthday

1. INTRODUCTION

Let E be an elliptic curve over $\mathbb{Q}$. By the rank of E we shall mean the rank of the group of rational points of E. Mestre [31], improving on the work of Néron [34] (cf. [13], [39] and [46]), has shown that there is an infinite family of elliptic curves over $\mathbb{Q}$ with rank at least 12. However, computational work (see [3], [4], [7] and [47]) suggests that a typical elliptic curve will have much smaller rank, with curves of rank 0 or 1 being predominant. Indeed, Brumer [6] has proved, subject to the Birch, Swinnerton-Dyer conjecture, the Shimura, Taniyama, Weil conjecture and the generalized Riemann hypothesis, that the average rank of an elliptic curve, ordered according to its Faltings height, is at most 2.3.

In this article we shall study the behaviour of the rank as we run over twists of a given elliptic curve over $\mathbb{Q}$. That is, we shall restrict our attention to families of elliptic curves defined over $\mathbb{Q}$ which are isomorphic over $\mathbb{C}$. There are families of quadratic, cubic, quartic and sextic twists (see, for example, Proposition 5.4 of Chapter X of [42]). Let E be an elliptic curve over $\mathbb{Q}$ with Weierstrass equation $y^2 = x^3 + ax + b$ and for any non-zero integer d let E_d denote a quadratic twist of E given by the equation $dy^2 = x^3 + ax + b$. Let $r(d)$ denote the rank of E_d. Note that if d_1 and d_2 are non-zero integers, then E_{d_1} is isomorphic to E_{d_2} over $\mathbb{Q}$ if and only if d_1/d_2 is the square of a rational number. Subject to the conjectures of Birch and Swinnerton-Dyer and of Shimura, Taniyama, and Weil, Goldfeld [14] conjectured in 1979 that

$$\sum_{0<|d|\le x} r(d) \sim \frac{1}{2} \sum_{0<|d|\le x} 1.$$

Further, in 1960 Honda [18] (see also [38], p. 162) conjectured that the rank of any twist of a given elliptic curve E over a number field K is bounded by a constant which depends on E and K only. Some related work on ranks of twists may be found in [12], [22] and [35].

Received by the editors July 30, 1992 and, in revised form, August 10, 1994.
1991 *Mathematics Subject Classification.* Primary 11G05, 11N36.
The first author's research was supported in part by a Killam Research Fellowship and by Grant A3528 from the Natural Sciences and Engineering Research Council of Canada.

In 1987, Zagier and Kramarz [47] examined cubic twists of the curve E given by the affine equation $x^3+y^3=1$. In particular they looked at the twists E_d of E given by the equation $x^3+y^3=d$. They calculated the value of the L-series of E_d and its derivative at 1 for all cube-free positive integers d less than 70,000. Subject to the Birch and Swinnerton-Dyer conjecture their calculations suggest that a positive proportion of the twists E_d of E have rank even and at least 2 and a positive proportion have rank odd and at least 3. The first theoretical results in this context are due to Gouvêa and Mazur [15]. Let E be an elliptic curve over $\mathbb{Q}$, given by $y^2=x^3+ax+b$. For any non-zero integer d let E_d denote the curve given by $dy^2=x^3+ax+b$ and let ε be a positive real number. For any real number T, let $S(T)$ denote the number of square-free integers d with $|d|\leq T$ for which the rank of E_d is even and at least 2. They proved, subject to the parity conjecture (see §12), that there are positive numbers C_0 and C_1, which depend on ε and E, such that whenever T exceeds C_0 then $S(T)$ is at least $C_1T^{\frac{1}{2}-\varepsilon}$. Thus, in the terminology of Gouvêa and Mazur, $\frac{1}{2}$ is an exponent for $S(T)$, subject to the parity conjecture. In [28], L. Mai extended the work of Gouvêa and Mazur to the case of cubic twists of $x^3+y^3=1$. He proved, subject to the parity conjecture for cubic twists (see §12), that for each positive real number ε there exist positive numbers C_2 and C_3, which depend on ε, such that for any real number T larger than C_2 the number of cube-free integers d with $|d|\leq T$ for which the rank of the curve given by $x^3+y^3=d$ is even and at least 2 is at least $C_3T^{\frac{2}{3}-\varepsilon}$.

Our aim in this paper is to generalize these results and to remove the dependence on the parity conjecture. Further we shall give a positive response to the question, posed by Gouvêa and Mazur [15], of whether there are positive exponents associated to functions counting the number of twists of an elliptic curve E which have rank larger than 2. For instance, we shall prove that there is a positive number C_4 such that if T is larger than 657, then the number of cube-free integers d with $|d|\leq T$ for which the curve given by $x^3+y^3=d$ has rank at least 3 is at least $C_4T^{\frac{1}{6}}$. Furthermore, by employing a construction of Mestre [30], we shall prove that if E is an elliptic curve over $\mathbb{Q}$ with j-invariant different from 0 and 1728 and, as usual, E_d denotes the quadratic twist of E, then there are positive numbers C_5 and C_6 which depend on E, such that if T exceeds C_5, then $S(T)$ is at least $C_6T^{\frac{1}{7}}/(\log T)^2$.

Our strategy will be to provide curves which are degree 2, 3, 4 and 6 cyclic covers of the projective line and which have the property that their jacobian contains over $\mathbb{Q}$, up to isogeny, many copies of a given elliptic curve. This method is not new, indeed Tate and Shafarevich [45] used it in the context of finite fields instead of $\mathbb{Q}$.

For any positive integer k and any integer n we say that n is k-free if n is not divisible by the kth power of a prime. To estimate the number of twists of large rank that our constructions yield we shall appeal to an estimate, of interest in its own right, for the number of k-free values below a given bound assumed by a binary form with integer coefficients evaluated at integer

arguments. Our result depends upon recent work of Greaves [16] who studied the related problem of estimating the number of pairs of integers (a, b) with $|a|$ and $|b|$ below a given bound for which $F(a, b)$ is k-free. To apply the work of Greaves we shall employ an argument due to Erdős and Mahler [11] and a result of Stewart [43] on the number of solutions of the Thue equation. Greaves' result sharpened work of Gouvêa and Mazur which in turn depended on a result of Hooley [19] which gives an asymptotic formula for the number of k-free positive integers up to x represented by an irreducible polynomial with integer coefficients of degree $k+1$ (≥ 3) and having no fixed kth power divisors.

Part of the research reported on here was done while the second author worked at Queen's University in Kingston, Ontario. During the remaining part he was employed by the Erasmus University in Rotterdam, the Netherlands. It is a pleasure to thank these institutions for their hospitality.

2. Strategy

Let E be an elliptic curve defined over $\mathbb{Q}$. Our aim is to construct many twists of E having large rank. To do so we shall regard E as an elliptic curve over $\mathbb{Q}(t)$. We shall study twists E_D of E where D is a polynomial in $\mathbb{Z}[t]$ of positive degree and where E_D and E are not isomorphic over $\mathbb{Q}(t)$ but become isomorphic over an extension $\mathbb{Q}(t, s)$ of $\mathbb{Q}(t)$ where $s^n = D(t)$ and n is 2, 3, 4 or 6 when we are considering quadratic, cubic, quartic or sextic twists respectively.

Our approach will be to first construct D so that the rank of the group of $\mathbb{Q}(t)$-points of E_D is large. Next we will appeal to a specialization argument to show that most specializations of t to a rational number give an elliptic curve over $\mathbb{Q}$ with rank at least as large as the rank of E_D over $\mathbb{Q}(t)$. Finally we shall use our result on n-free values assumed by binary forms to count the number of different twists we get by specializing. The binary form $F(X, Y)$ which we will arrive at is given by $F(X, Y) = Y^l D(\frac{X}{Y})$ where l is the smallest multiple of n greater than or equal to the degree of D.

3. Specialization

Let E be an elliptic curve defined over $\mathbb{Q}(t)$ which is not isomorphic over $\mathbb{Q}(t)$ to an elliptic curve defined over $\mathbb{Q}$. By specializing t to a rational number t_0 one obtains in general an elliptic curve $E_{t_0}/\mathbb{Q}$ and a specialization homomorphism $\rho_{t_0}: E(\mathbb{Q}(t)) \to E_{t_0}(\mathbb{Q})$ from the group of $\mathbb{Q}(t)$-points of E to the group of rational points of E_{t_0}. We shall make use of the following result due to Silverman.

Lemma 1. *In the above situation,*

$$\rho_{t_0}: E(\mathbb{Q}(t)) \to E_{t_0}(\mathbb{Q})$$

is an injective homomorphism for all but finitely many rational numbers t_0.

Proof. This is a special case of Theorem C of [40]; one takes the abelian variety to be an elliptic curve.

4. Calculation of the rank of E_D over $\mathbb{Q}(t)$

Let $D(t)$ be a polynomial with integer coefficients and degree at least 1 and let n be an integer larger than 1. Suppose that D is not a perfect pth power in $\mathbb{C}[t]$ for any prime p which divides n. Let C be a smooth, complete model of the curve given by $s^n = D(t)$ and let $H^0(C, \Omega^1_{C/\mathbb{Q}})$ denote the vector space of holomorphic differentials on C. Let E be an elliptic curve. We denote the set of morphisms from C to E defined over $\mathbb{Q}$ by $\mathrm{Mor}_{\mathbb{Q}}(C, E)$ and give it the structure of an abelian group by defining the sum of two morphisms φ_1 and φ_2 to be the morphism which takes x in C to $\varphi_1(x) + \varphi_2(x)$ where $+$ denotes addition in E.

Proposition 1. *Consider the following four situations.*

1. (quadratic twists) *$E/\mathbb{Q}$ is an elliptic curve given by an equation $y^2 = ax^3 + bx^2 + cx + d$ and $D \in \mathbb{Z}[t]$ is a non-constant polynomial which is not a perfect square in $\mathbb{C}[t]$. $C/\mathbb{Q}$ is a smooth, complete model of the curve defined by $s^2 = D(t)$ and $E_D/\mathbb{Q}(t)$ is given by $D(t)y^2 = ax^3 + bx^2 + cx + d$.*

For each point $P = (x(t), y(t))$ in $E_D(\mathbb{Q}(t))$ we define an element φ_P of $\mathrm{Mor}_{\mathbb{Q}}(C, E)$ by $\varphi_P(t, s) = (x(t), sy(t))$.

2. (cubic twists) *$E/\mathbb{Q}$ is an elliptic curve given by an equation $y^2 = x^3 + k$ and $D \in \mathbb{Z}[t]$ is a non-constant polynomial which is not a perfect cube in $\mathbb{C}[t]$. $C/\mathbb{Q}$ is a smooth, complete model of the curve defined by $s^3 = D(t)$ and $E_D/\mathbb{Q}(t)$ is given by $y^2 = x^3 + k(D(t))^2$.*

For each point $P = (x(t), y(t))$ in $E_D(\mathbb{Q}(t))$ we define an element φ_P of $\mathrm{Mor}_{\mathbb{Q}}(C, E)$ by $\varphi_P(t, s) = (x(t)s^{-2}, y(t)s^{-3})$.

3. (quartic twists) *$E/\mathbb{Q}$ is an elliptic curve given by an equation $y^2 = x^3 + ax$ and $D \in \mathbb{Z}[t]$ is a non-constant polynomial which is not a perfect square in $\mathbb{C}[t]$. $C/\mathbb{Q}$ is a smooth complete model of the curve defined by $s^4 = D(t)$ and $E_D/\mathbb{Q}(t)$ is given by $y^2 = x^3 + aD(t)x$.*

For each point $P = (x(t), y(t))$ in $E_D(\mathbb{Q}(t))$ we define an element φ_P of $\mathrm{Mor}_{\mathbb{Q}}(C, E)$ by $\varphi_P(t, s) = (x(t)s^{-2}, y(t)s^{-3})$.

4. (sextic twists) *$E/\mathbb{Q}$ is an elliptic curve given by an equation $y^2 = x^3 + k$ and $D \in \mathbb{Z}[t]$ is a non-constant polynomial which is not a perfect square or a perfect cube in $\mathbb{C}[t]$. $C/\mathbb{Q}$ is a smooth, complete model of the curve defined by $s^6 = D(t)$ and $E_D/\mathbb{Q}(t)$ is given by $y^2 = x^3 + kD(t)$.*

For each point $P = (x(t), y(t))$ in $E_D(\mathbb{Q}(t))$ we define an element φ_P of $\mathrm{Mor}_{\mathbb{Q}}(C, E)$ by $\varphi_P(t, s) = (x(t)s^{-2}, y(t)s^{-3})$.

In each of the above four cases the map

$$\lambda: E_D(\mathbb{Q}(t)) \to H^0(C, \Omega^1_{C/\mathbb{Q}})$$

given by

$$\lambda(P) = \varphi_P^* \omega_E,$$

where $\varphi_P^* \omega_E$ denotes the pullback via φ_P of the invariant differential ω_E on E, is a homomorphism with a finite kernel.

Proof. We shall first prove that λ is a homomorphism. Observe that $\lambda = \lambda_2 \circ \lambda_1$ where $\lambda_1 : E_D(\mathbb{Q}(t)) \to \mathrm{Mor}_{\mathbb{Q}}(C, E)$ by $\lambda_1(P) = \varphi_P$ and $\lambda_2 : \mathrm{Mor}_{\mathbb{Q}}(C, E) \to H^0(C, \Omega^1_{C/\mathbb{Q}})$ by $\lambda_2(\varphi) = \varphi^* \omega_E$. In all four cases λ_1 is a homomorphism as may be verified by appealing to the addition law on E and on E_D. Also λ_2 is a homomorphism as may be confirmed as in the proof of Theorem 5.2 of Chapter III of [42].

To see that λ has a finite kernel notice that only constant morphisms yield a vanishing pullback of ω_E. The result then follows in each case.

Observe that, by the proof of Proposition 1, polynomials D for which the rank of $E_D(\mathbb{Q}(t))$ is large will have many independent morphisms from C to E of the appropriate form.

We shall use Proposition 1 to establish lower bounds for the rank of $E_D(\mathbb{Q}(t))$ for various curves $E_D/\mathbb{Q}(t)$ as above. To do so we shall start with a set of points in $E_D(\mathbb{Q}(t))$. Then it is a straightforward task to calculate the rank of the group generated by the image under λ of these points in the vector space of holomorphic differentials on C. Since λ is a homomorphism this rank is a lower bound for the rank of $E_D(\mathbb{Q}(t))$.

Let D, n and C be defined as at the start of this section. Let ζ_n be a primitive nth root of unity and define ζ, an automorphism of C, by $\zeta(t, s) = (t, \zeta_n s)$. Then ζ acts on the differentials of C via the pullback $\zeta^* f(t, s)\, dt = f(t, \zeta_n s)\, dt$ for any function f on C. Hence one obtains a linear action on the space $H^0(C, \Omega^1_{C/\mathbb{Q}})$ of holomorphic differentials on C. This action yields a decomposition

$$H^0(C, \Omega^1_{C/\mathbb{Q}}) = \bigoplus_{i=0}^{n-1} H^0(C, \Omega^1_{C/\mathbb{Q}})(\zeta_n^i),$$

in which $H^0(C, \Omega^1_{C/\mathbb{Q}})(\zeta_n^i)$ is the eigenspace on which ζ acts by multiplication by ζ_n^i.

Corollary 1. *Consider the four situations of Proposition* 1. *For each case we have*

$$\mathrm{rank}\, E_D(\mathbb{Q}(t)) \leq \dim H^0(C, \Omega^1_{C/\mathbb{Q}})(\zeta_n).$$

Proof. We check in each of the four cases that $\varphi_P^* \omega_E$ has the form $r(t)s\,dt$ where $r(t)$ is a rational function of t. Thus $\varphi_P^* \omega_E$ is in $H^0(C, \Omega^1_{C/\mathbb{Q}})(\zeta_n)$ and our first assertion now follows from Proposition 1 since the kernel of λ is finite.

We remark that the term on the right-hand side of the above inequality is equal to $\mathrm{Hom}_{\mathbb{Q}}(\mathrm{Jac}(C), E)$.

5. Power-free values of binary forms

Let

$$F(X, Y) = a_r X^r + a_{r-1} X^{r-1} Y + \cdots + a_0 Y^r \tag{1}$$

be a binary form with integer coefficients and positive degree r. Let A, B, M and k be integers with $M \geq 1$ and $k \geq 2$. We shall now define three counting functions associated with k-free values of F. We shall include the congruence condition $X \equiv A \pmod{M}$ and $Y \equiv B \pmod{M}$ in the definition of these functions since such a condition is required for applications involving the parity conjecture (see §12). It is also useful when one wishes to estimate the number of fields with discriminant in absolute value below a given bound and for which the ideal class group is of a certain type. Let w be the largest positive integer such that w^k divides $F(a, b)$ for all integers a and b with $a \equiv A \pmod{M}$ and $b \equiv B \pmod{M}$. For any real number x let $N_k(x)$ and $P_k(x)$ denote the number of pairs of integers (a, b) with $1 \leq a \leq x$, $1 \leq b \leq x$, $a \equiv A \pmod{M}$ and $b \equiv B \pmod{M}$ for which $F(a, b)$ is k-free and for which $F(a, b)/w^k$ is k-free respectively. For any real number x let $R_k(x)$ denote the number of k-free integers t with $|t| \leq x$ for which there are integers a and b with $a \equiv A \pmod{M}$, $b \equiv B \pmod{M}$ and $F(a, b) = tw^k$.

Let f be a polynomial with integer coefficients which is irreducible over the rational numbers. Let r denote the degree of f and suppose that r is at least 3. For any real number x let $N(f, r-1, x)$ denote the number of positive integers n not exceeding x for which $f(n)$ is $(r-1)$-free. Hooley [19], [20] proved that

$$N(f, r-1, x) = C_7 x + O(x(\log x)^{(2/(r+1))-1}),$$

where C_7 is a non-negative number which depends on f and r and which is positive when f has no fixed $(r-1)$th power divisor larger than 1. Let F be a binary form as in (1). Suppose that F has non-zero discriminant, $a_r a_0 \neq 0$, and that all of the irreducible factors of F over $\mathbb{Q}$ have degree at most 3. Gouvêa and Mazur adapted the sieving argument of Hooley to prove that

$$N_2(x) = C_8 x^2 + O(x^2/(\log x)^{\frac{1}{2}}), \tag{2}$$

where C_8 is a non-negative number which depends on A, B, M and F. To count the number of distinct quadratic twists of an elliptic curve given by $Y^2 = X^3 + aX + b$ which their construction yields they need a corresponding result for $R_2(x)$. Suppose that M is a positive integer, a and b are integers divisible by M and that $4a^3 + 27b^2 \neq 0$. Let $F(X, Y) = Y(X^3 + aXY^2 + bY^3)$ and let A and B be integers coprime with M. For any non-zero integer h the number of pairs of integers (s, t) with $F(s, t) = h$ is, since Y is a factor of F, at most $3\tau(h)$ where $\tau(h)$ denotes the number of positive integers which divide h. Using this fact and their result on $N_2(x)$ they deduce, in the special case above, that for each positive real number ε there are positive numbers C_9 and C_{10} which depend on ε, a, b, A, B and M such that if x is a real number larger than C_9, then

$$R_2(x) > C_{10} x^{\frac{1}{2}-\varepsilon}.$$

In a recent article Greaves [16] improved on the result (2) of Gouvêa and Mazur. Let F, A, B, M and k be as in the introduction to this section. Define w_0 to be the largest positive integer such that w_0^k divides $F(a, b)$ for all integers a and b. Let m denote the degree of the largest irreducible factor

of F over $\mathbb{Q}$. Greaves assumes that F has non-zero discriminant, $a_r a_0 \neq 0$ and $w_0 = 1$. He then proves that there is a non-negative number C_{11}, which depends on M, A, B and F, such that if $]m \leq 6$, then

$$N_2(x) = C_{11}x^2 + O(x^2/(\log x)^{\frac{1}{3}})$$

and there is a non-negative number C_{12}, which depends on M, A, B, F and k, such that if $m \leq 2k+1$, then

$$N_k(x) = C_{12}x^2 + O(x^2/\log x);$$

here the O-constants depend only on F. Further he proves that if $M = 1$, then C_{11} and C_{12} are positive.

Our aim is to prove corresponding results for $R_k(x)$. As a first step we shall modify the arguments of Greaves so that they apply to the functions $P_k(x)$. Again let F, A, B, M and k be as in the introduction to this section. For each prime p let $\mathrm{ord}_p t$ denote the p-adic order of t. Put $m = \mathrm{ord}_p M$, $v = \mathrm{ord}_p w^k$ and $l = k + m + v$. Let S be the set of those primes which divide M, w, or the discriminant of F. Let $s(p)$ denote the number of pairs of integers (a, b) with $1 \leq a \leq p^l$, $1 \leq b \leq p^l$, $a \equiv A \pmod{p^m}$, $b \equiv B \pmod{p^m}$ and for which $F(a, b) \not\equiv 0 \pmod{p^{k+v}}$. Put

$$C_{13} = \prod_p \frac{s(p)}{p^{2l}}. \tag{3}$$

(The authors would like to thank Professor M. Filaseta for his comments concerning the definition of C_{13}.) The number of pairs (a, b) with $1 \leq a \leq p^k$ and $1 \leq b \leq p^k$ for which p divides both a and b is p^{2k-2}. Further the number of pairs (a, b) with $1 \leq a \leq p^k$, $1 \leq b \leq p^k$, for which p does not divide both a and b and for which $F(a, b) \equiv 0 \pmod{p^k}$, is at most rp^k provided that p does not divide the discriminant of F (see, for example, Theorem 2 of [43]). Thus

$$s(p) \geq p^{2k} - p^{2k-2} - rp^k \tag{4}$$

for primes p which are not in S. It follows from the definition of w that $s(p) \geq 1$ for all primes p. Therefore the product defining C_{13} converges to a positive real number.

Lemma 2. *Let A, B, M, F, k and w be defined as in the introduction to this section. Suppose that F has non-zero discriminant, $a_r a_0 \neq 0$ and that m denotes the degree of the largest irreducible factor of F over $\mathbb{Q}$. If $m \leq 6$, then*

$$P_2(x) = C_{13}x^2 + O(x^2/(\log x)^{\frac{1}{3}})$$

while if $m \leq 2k+1$, then

$$P_k(x) = C_{13}x^2 + O(x^2/\log x),$$

where the O-constants depend only on F, M and k.

Proof. Put $\lambda = (\log x)/2k$ and assume that x is sufficiently large that

$$\prod_{p \leq \lambda} p^l \leq x^{\frac{2}{3}}, \tag{5}$$

that all primes p in S are less than λ and that all primes which divide $a_r a_0$ are also less than λ.

We suppose that $F(X, Y) = \prod_{i=1}^{t} F_i(X, Y)$ where the forms F_i have integer coefficients and are irreducible in $\mathbb{Q}[X, Y]$. Let $E_0(x)$ denote the number of pairs of integers (a, b) with $1 \leq a \leq x$ and $1 \leq b \leq x$ for which p divides both a and b for some prime p with $p > \lambda$. For $i = 1, \ldots, t$ let $E_i(x)$ denote the number of pairs (a, b) with $1 \leq a \leq x$ and $1 \leq b \leq x$ for which there is a prime p larger than λ which does not divide both a and b and for which p^k divides $F_i(a, b)$. Put

$$V = \prod_{p \leq \lambda} p^l,$$

and for integers i and j denote the set of pairs of integers (a, b) with $iV < a \leq (i+1)V$ and $jV < b \leq (j+1)V$ by $W_{i,j}$. Notice that the set of pairs (a, b) with $1 \leq a \leq x$ and $1 \leq b \leq x$ contains the union of the sets $W_{i,j}$ with $0 \leq i, j \leq [\frac{x}{V}] - 1$ and is contained in the union of these sets with $0 \leq i, j \leq [\frac{x}{V}]$. Thus, by the Chinese Remainder Theorem, and (5),

$$P_k(x) = \left(\prod_{p \leq \lambda} \frac{s(p)}{p^{2l}} \right) x^2 + O(x^{\frac{5}{3}}) + O\left(\sum_{i=0}^{t} E_i(x) \right)$$

and so, by (4),

$$P_k(x) = C_{13} x^2 + O(x^2 / \log x) + O\left(\sum_{i=0}^{t} E_i(x) \right);$$

here the O-constants depend on F, M and k.

It only remains to estimate the error terms $E_i(x)$ for $i = 0, \ldots, t$. This is done in [16] by Greaves with $\lambda = \frac{1}{3} \log x$. Moreover Greaves' argument works equally well with $\lambda = (\log x)/2k$; only a minor modification is required in the proof of Lemma 2 of [16] where the terms $E_i^{(1)}(x)$ are estimated. The result now follows.

Let F be a binary form, as in (1), with integer coefficients, non-vanishing discriminant, degree r at least 3 and $a_r a_0 \neq 0$. For any integer x let $R(x)$ denote the number of integers t with $|t| \leq x$ for which there exist integers a and b with $F(a, b) = t$. In 1938 Erdős and Mahler [11] proved that there is a positive number C_{14}, which depends on F, such that for x sufficiently large

$$R(x) > C_{14} x^{\frac{2}{r}}.$$

Mahler [27] has shown that this estimate is best possible apart from the number C_{14}. We shall modify the argument of Erdős and Mahler in order to estimate the number of distinct k-free integers t of absolute value at most x for which there are integers a and b with $F(a, b) = t$.

Theorem 1. *Let A, B, M and k be integers with $M \geq 1$ and $k \geq 2$. Let F, as in (1), be a binary form with integer coefficients, non-zero discriminant and degree r with $r \geq 3$. Let m be the largest degree of an irreducible factor of F*

over $\mathbb{Q}$ *and suppose that* $m \leq 2k+1$ *or that* $k = 2$ *and* $m = 6$. *There are positive numbers* C_{15} *and* C_{16} *which depend on* M, k *and* F, *such that if* x *is a real number larger than* C_{15}, *then*

$$R_k(x) > C_{16} x^{\frac{2}{r}}.$$

Erdős and Mahler appealed to a modification of Mahler's [26] p-adic version of the Thue-Siegel theorem to establish their result. We have found it convenient to appeal to a recent result of Stewart [43] on the number of solutions of the Thue equation for the proof of Theorem 1, although we could also get by with Mahler's result or Lemma 8 of [11]. In fact the full power of these results is not needed since in the proof of Theorem 1 we only need an estimate for relatively small solutions of the Thue equations involved and an argument based on a gap principle suffices for this purpose. Thus the Thue-Siegel principle (see [43]) is not required.

6. Proof of Theorem 1

We may assume that $k \leq r$ since m is at most r and since if an integer is k-free it is also $(k+1)$-free. We may also assume, without loss of generality, that $a_r a_0 \neq 0$. To see this note that if $a_r a_0 = 0$, then there is a matrix

$$\mathcal{M} = \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix}$$

in $SL(2, \mathbb{Z})$ for which $F(m_1X + m_2Y, m_3X + m_4Y) = a_r'X^r + a_{r-1}'X^{r-1}Y + \cdots + a_0'Y^r$ with $a_r'a_0' \neq 0$. Denote $F(m_1X+m_2Y, m_3X+m_4Y)$ by $F_{\mathcal{M}}(X, Y)$. Since $\mathcal{M}$ is in $SL(2, \mathbb{Z})$ the discriminant of $F_{\mathcal{M}}$ is the same as the discriminant of F. Further let $A' = m_1A + m_2B$ and $B' = m_3A + m_4B$ and observe that the set of integers of the form $F_{\mathcal{M}}(a, b)$ with $a \equiv A' \pmod{M}$ and $b \equiv B' \pmod{M}$ is the same as the set of integers of the form $F(a, b)$ with $a \equiv A \pmod{M}$ and $b \equiv B \pmod{M}$. Accordingly, we may replace F by $F_{\mathcal{M}}$ if necessary.

For any prime p and any rational number a let $|a|_p$ denote the p-adic value of a, normalized so that $|p|_p = p^{-1}$. Let u be a positive real number. For any real number θ with $0 < \theta \leq 1$ and for any non-zero integer h we define $s(h)$ by

$$s(h) = \prod_{\substack{p \leq u^\theta \\ |h|_p^{-1} \leq u^\theta \\ p \nmid wD}} |h|_p^{-1},$$

where D denotes the discriminant of F. Let U denote the set of pairs of integers (a, b) with $1 \leq a \leq u$, $1 \leq b \leq u$ and $F(a, b) \neq 0$ and such that the only primes which divide the greatest common divisor of a and b also divide wD. Next we define $S(\theta, u)$ by

$$S(\theta, u) = \prod_{(a,b) \in U} s(F(a, b)).$$

We shall now estimate $S(\theta, u)$ by an argument similar to that of Lemma 1 of [11]. Note, however, that the proof of Lemma 1 of [11] is incorrect as it stands since the authors do not give a valid estimate for $\mathrm{ord}_p G$. They overlook the contribution from pairs (x, y) for which p divides both x and y. This can be easily fixed by requiring that the pairs (x, y) in the product defining G are pairs of coprime integers. The balance of their argument goes through unchanged.

Let p be a prime which does not divide wD and let z be a positive integer for which $p^z \leq u^\theta$. Note that the content of F divides D. For each integer b which is coprime with p there are at most r integers a modulo p^z for which

$$F(a, b) \equiv 0 \pmod{p^z}. \tag{6}$$

Thus there are at most $ru([\frac{u}{p^z}]+1)$ solutions of (6) from U for which p does not divide b. The same estimate applies for the number of solutions of (6) from U for which p does not divide a. Thus

$$\mathrm{ord}_p S(\theta, u) \leq \sum_{z=1}^{[\frac{\theta \log u}{\log p}]} \frac{4ru^2}{p^z} \leq \sum_{z=1}^{\infty} \frac{4ru^2}{p^z} = \frac{4ru^2}{p-1}.$$

Therefore

$$S(\theta, u) \leq \exp\left(4ru^2 \sum_{\substack{p \leq u^\theta \\ p \nmid wD}} \frac{\log p}{p-1}\right).$$

Hence, by Theorem 425 of [17], there is a positive number C_{17}, which depends on θ, such that if u exceeds C_{17}, then

$$S(\theta, u) \leq u^{5\theta ru^2}.$$

Consequently, if u exceeds C_{17}, the number of pairs (a, b) in U for which $s(F(a, b)) \geq u^{\frac{1}{8}}$ is at most

$$40\theta ru^2. \tag{7}$$

Next observe, as in Lemma 2 of [11], that if h and b are integers with $|h| \leq u^{\frac{1}{2}}$ and $1 \leq b \leq u$, then there are at most r integers a with $F(a, b) = h$. Accordingly, the number of pairs of integers (a, b) with $1 \leq a \leq u$, $1 \leq b \leq u$ and $|F(a, b)| \leq w^r u^{\frac{1}{2}}$ is at most

$$3rw^r u^{\frac{3}{2}}. \tag{8}$$

We now fix θ by putting

$$\theta = C_{13}/120r; \tag{9}$$

recall (3). Let T be the set of pairs of integers (a, b) with $1 \leq a \leq u$, $1 \leq b \leq u$, $a \equiv A \pmod{M}$, $b \equiv B \pmod{M}$ and for which $F(a, b)/w^k$ is k-free, $|F(a, b)| \geq w^r u^{\frac{1}{2}}$ and $s(F(a, b)) < u^{\frac{1}{8}}$. Note that if $F(a, b)/w^k$ is k-free, then, since $k \leq r$, the greatest common divisor of a and b divides w.

Thus T is contained in U. For any set X we denote the cardinality of X by $|X|$. By Lemma 2, (7), (8) and (9) there are positive numbers C_{18} and C_{19}, which depend on F, M and k, such that if u exceeds C_{18}, then

$$|T| > \tfrac{1}{2}C_{13}u^2. \tag{10}$$

As we remarked above, if (a, b) is in T, then the greatest common divisor of a and b divides w. Let d be that divisor of w which occurs most often as the greatest common divisor of a pair (a, b) from T. Let T_0 be the set of pairs (a, b) from T whose greatest common divisor is d and let T_1 be the set of pairs $(\frac{a}{d}, \frac{b}{d})$ with (a, b) in T_0. It follows from (10) that

$$|T_1| > C_{13}u^2/(2\tau(w)), \tag{11}$$

provided that u exceeds C_{18}. Observe that if (a', b') is in T_1, then a' and b' are coprime, $1 \le a' \le u$, $1 \le b' \le u$, $|F(a', b')| \ge u^{\frac{1}{2}}$ and $s(F(a', b')) < u^{\frac{1}{8}}$.

For any non-zero integer h let $\omega(h)$ denote the number of distinct prime factors of h. Let h be an integer for which there is a pair (a', b') in T_1 with

$$F(a', b') = h. \tag{12}$$

Put $h = s(F(a', b')) \cdot g$ and note that $|g| \ge |h|^{\frac{3}{4}}$. If u is larger than $|D|^{24}$, then h is larger than $|D|^{12}$ and so, on taking $\varepsilon = 1/12$ in Corollary 1 of [43], we deduce that the number of pairs (a', b') from T_1 for which (12) holds is at most

$$5600r^{1+\omega(g)}. \tag{13}$$

Let H denote the maximum of $\{|a_0|, \ldots, |a_r|\}$ and observe that if (a', b') is in T_1, then

$$|F(a', b')| \le rHu^r. \tag{14}$$

The prime divisors p of g either divide wD or satisfy $|F(a', b')|_p^{-1} \ge u^{\theta}$. Thus, provided that $u^{\theta} \ge rH$,

$$\omega(g) \le \omega(wD) + (r+1)/\theta. \tag{15}$$

Therefore, by (9), (11), (13) and (15) there are positive numbers C_{20} and C_{21}, which depend on F, M and k, such that if u exceeds C_{20}, then the number of distinct integers h of the form $F(a', b')$ with (a', b') in T_1 is at least $C_{21}u^2$ and so the number of distinct integers $F(a, b)$ with (a, b) in T is also at least $C_{21}u^2$.

Let x be a real number with $x > rHC_{20}^r$ and put $u = (x/rH)^{\frac{1}{r}}$; note that u exceeds C_{20}. We now define T as above and observe that if (a, b) is in T, then $|F(a, b)| \le x$. Thus

$$R_k(x) \ge |T| \ge C_{21}(x/rH)^{\frac{2}{r}},$$

and this completes the proof of Theorem 1.

7. Values of binary forms modulo k th powers

Let A, B, M and k be integers with $M \geq 1$ and $k \geq 2$. Let F be a binary form as in (1). For any real number x let $S_k(x)$ denote the number of k-free integers t with $|t| \leq x$ for which there exist integers a, b and z with $a \equiv A \pmod{M}$, $b \equiv B \pmod{M}$, z non-zero and $F(a, b) = tz^k$. It is the function $S_k(x)$ which we use to count the number of different twists of elliptic curves produced by our constructions. Plainly we have

$$S_k(x) \geq R_k(x),$$

and so the estimate for $R_k(x)$ given by Theorem 1 furnishes a lower bound for $S_k(x)$ provided that the hypotheses of Theorem 1 apply. Our next result gives a weaker lower bound for $S_k(x)$ which, however, is more widely applicable.

Our first version of this result gave a lower bound for $S_k(x)$ of $C_{23}x^{1/r}/\log x$. Professor A. Granville pointed out to us how to improve this to $C_{23}x^{2/r}/(\log x)^2$. We are very grateful to him for allowing us to incorporate his ideas into our proof.

Theorem 2. *Let A, B, M and k be integers with $M \geq 1$ and $k \geq 2$. Let F be a binary form with integer coefficients and degree r which is not a constant multiple of a power of a linear form and which is not divisible over $\mathbb{Q}$ by the kth power of a non-constant binary form. There are positive numbers C_{22} and C_{23}, which depend on F and M, such that if x is a real number larger than C_{22}, then*

$$S_k(x) > C_{23}x^{\frac{2}{r}}/(\log x)^2.$$

Proof. $C_{24}, C_{25}, \ldots$ will denote positive numbers which are effectively computable in terms of F and M. We may write $F(X, Y) = F_1(X, Y) \cdots F_l(X, Y)$ where $F_1, \ldots, F_l$ are binary forms with integer coefficients, F_{i+1} divides F_i for $i = 1, \ldots, l-1$ and F_i is either linear or has a non-zero discriminant for $i = 1, \ldots, l$. Since F is not divisible by the kth power of a non-constant binary form, l is at most $k-1$. Next we write $F_1(X, Y) = G_1(X, Y) \cdots G_m(X, Y)$ where $G_1, \ldots, G_m$ are non-constant forms with integer coefficients which are irreducible in $\mathbb{Q}[X, Y]$.

We first deal with the case that one of $G_1, \ldots, G_m$ is non-linear. We may assume without loss of generality that G_1 is non-linear. Put $G(X) = G_1(X, 1)$ for brevity.

Let u be a positive real number for which $u/2$ exceeds the maximum of M, the content of F and the discriminant of F_1. Let W be the set of primes p with $u/2 < p < u$ for which the congruence $G(X) \equiv 0 \pmod{p}$ has a solution. By the Chebotarev density theorem [24] there are positive numbers C_{24} and C_{25} such that if u exceeds C_{24}, then

$$|W| > C_{25}u/\log u.$$

Let p be a prime in W and let v be an integer with $0 \leq v < p$ for which $G(v) \equiv 0 \pmod{p}$, hence for which $F_1(v, 1) \equiv 0 \pmod{p}$. Since p is larger than $u/2$, p does not divide the content or the discriminant of F_1. Thus, by Hensel's lemma, there is a unique integer v_1 with $0 \leq v_1 < p$ such that

if $x \equiv v \pmod{p}$ and $F_1(x, 1) \equiv 0 \pmod{p^2}$, then $x \equiv v + v_1 p \pmod{p^2}$. We have $F_1(r, s) \equiv 0 \pmod{p}$ whenever (r, s) is a pair of integers with $r \equiv vs \pmod{p}$. The set of such pairs (r, s) forms a lattice Λ_p of determinant p. Further the set of pairs (r, s) in Λ_p for which $F_1(r, s) \equiv 0 \pmod{p^2}$ forms a sublattice of determinant p^2.

Let (r_0, s_0) be an element of Λ_p different from $(0, 0)$ for which $\max(|r_0|, |s_0|)$ is minimal and put $m_p = \max(|r_0|, |s_0|)$. Let d denote the degree of G_1. There exists a positive number C_{26} such that whenever (r, s) is in Λ_p with $(r, s) \neq (0, 0)$, then

$$0 < |G_1(r, s)| < C_{26}(\max(|r|, |s|))^d; \tag{16}$$

note that $G_1(r, s)$ is non-zero since G_1 is irreducible and of degree at least two. Thus if u exceeds C_{27} and the maximum of $|r|$ and $|s|$ is at most $u^{\frac{1}{2}}$, then at most d primes from W divide $G_1(r, s)$. If u exceeds C_{28} the number of pairs of integers (r, s) with

$$\max(|r|, |s|) < (C_{25}u/(10d \log u))^{\frac{1}{2}}$$

is at most $C_{25}u/(2d \log u)$. Accordingly, by inequality (16), there are at most $C_{25}u/(2 \log u)$ primes p in W for which m_p is less than $(C_{25}u/(10d \log u))^{\frac{1}{2}}$. Let W_1 be the set of primes p in W for which

$$m_p \geq (C_{25}u/(10d \log u))^{\frac{1}{2}}, \tag{17}$$

and note that

$$|W_1| \geq C_{25}u/(2 \log u). \tag{18}$$

Let p be a prime in W_1 and let (r_0, s_0) and (r_1, s_1) be a basis for Λ_p with $\max(|r_1|, |s_1|)$ minimal. It follows from (17), as in Lemma 1 of [16] (see in particular (2.8) of [16]), that

$$\max(|r_0|, |s_0|, |r_1|, |s_1|) \leq C_{29}(u \log u)^{\frac{1}{2}}. \tag{19}$$

Since M and p are coprime and the determinant $|r_0 s_1 - r_1 s_0|$ of Λ_p is p, there exist integers j and k with $0 \leq j < M$ and $0 \leq k < M$ for which $jr_0 + kr_1 \equiv A \pmod{M}$ and $js_0 + ks_1 \equiv B \pmod{M}$. Put $(r_2, s_2) = j(r_0, s_0) + k(r_1, s_1)$, $(r_3, s_3) = (r_2, s_2) + M(r_0, s_0)$ and $(r_4, s_4) = (r_2, s_2) + M(r_1, s_1)$. Note that $r_i \equiv A \pmod{M}$, $s_i \equiv B \pmod{M}$ and $F_1(r_i, s_i) \equiv 0 \pmod{p}$ for $i = 2, 3$ and 4. Further, we can find two linearly independent vectors in $\{(r_2, s_2), (r_3, s_3), (r_4, s_4)\}$ and these two vectors generate a sublattice of Λ_p of determinant at most $C_{30}u \log u$ by virtue of (19). Since the set of pairs (r, s) in Λ_p for which $F_1(r, s) \equiv 0 \pmod{p^2}$ forms a sublattice of Λ_p of determinant p^2 and p^2 exceeds $u^2/4$ we see that $\operatorname{ord}_p F_1(r_i, s_i) = 1$ when i is 2, 3 or 4 provided that u exceeds C_{31}. Thus for each prime p in W_1 there exists a pair of integers (a, b) with

$$a \equiv A \pmod{M}, \qquad b \equiv B \pmod{M}, \qquad \operatorname{ord}_p F_1(a, b) = 1 \tag{20}$$

and

$$\max(|a|, |b|) \leq C_{32}(u \log u)^{\frac{1}{2}}. \tag{21}$$

Assume that F is as in (1) and put $H = \max\{|a_r|, \ldots, |a_0|\}$. Then put $u = (x/rH)^{\frac{2}{r}}/(C_{32}^2 \log x)$ so that when x exceeds C_{33} and (21) holds, then $|F(a, b)| \leq x$. Observe that, by (18),

$$|W_1| > C_{34}x^{\frac{2}{r}}/(\log x)^2. \tag{22}$$

To each prime p in W_1 there exists a pair of integers (a, b) satisfying (20) and with $|F(a, b)| \leq x$. Put $F(a, b) = t_p z^k$ where t_p and z are integers with t_p k-free and z positive. Next put $T = \{t_p | p \in W_1\}$. Since l is less than k, we have

$$1 \leq \operatorname{ord}_p F(a, b) < k,$$

and therefore p divides t_p for each prime p in W_1. Further for each integer t in T we have $|t| \leq x$. Furthermore, for each integer t in T there are at most r primes p from W_1 with $t_p = t$ provided that u exceeds C_{35}, since each prime p in W_1 exceeds $u/2$. Thus

$$S_k(x) \geq |T| \geq |W_1|/r,$$

and the result follows from (22).

We are left with the case where $G_1, \ldots, G_m$ are linear forms. We first treat the case when m is at least three. As before let w be the largest integer such that w^2 divides $F_1(a, b)$ for all integers a and b with $a \equiv A \pmod{M}$ and $b \equiv B \pmod{M}$. Let u be a positive real number and define T to be the set of integers $F_1(a, b)$ with $1 \leq a \leq u$, $1 \leq b \leq u$, $a \equiv A \pmod{M}$, $b \equiv B \pmod{M}$ and $F_1(a, b)/w^2$ square-free. It is established in the penultimate paragraph of the proof of Theorem 1 that there exists a positive number C_{36} such that if u exceeds C_{36}, then $|T|$ is at least $C_{37}u^2$. If $F_1(a, b)$ is in T and p is a prime which divides $F_1(a, b)$ but does not divide w, then

$$1 \leq \operatorname{ord}_p F(a, b) < k.$$

Put $u = (x/rH)^{\frac{1}{r}}$ and note that $|F(a, b)|$ is at most x when the maximum of $|a|$ and $|b|$ is at most u. Therefore

$$S_k(x) \geq |T|/2^{\omega(w)} \geq C_{38}x^{\frac{2}{r}},$$

when x is at least C_{39}.

Finally we must deal with the possibility that F_1 is the product of two linear forms. We may suppose that $F_1(X, Y) = (cX + dY)(eX + fY)$ with $c, d, e,$ and f integers. Since $cX + dY$ and $eX + fY$ are non-proportional, we may assume that c is non-zero. Put $a = A + kM$ and $b = B + lcM$ so that

$$F_1(a, b) = (cA + dB + (k + dl)cM)(eA + fB + (ek + cfl)M).$$

Let S_1 denote the greatest common divisor of $cA + dB$ and cM. Then by the prime number theorem for arithmetic progressions with error term, if u

is a real number larger than C_{40}, then the number of primes p of the form $((cA + dB)/S_1 + t(cM/S_1))$ with t an integer and $u/2 < p < u$ is at least $C_{41}u/\log u$. For each integer t as above we put $k = t - dl$ so that we have $(eA + fB + (ek + cfl)M) = (eA + fB + etM + (cf - de)lM)$. Let S_2 be the greatest common divisor of $eA + fB + etM$ and $(cf - de)M$. Then, again by the prime number theorem for arithmetic progressions with error term, if u is a real number larger than C_{42}, then the number of primes p of the form

$$((eA + fB + etM)/S_2 + ((cf - de)M/S_2)l)$$

with l an integer and $u < p < 2u$ is at least $C_{43}u/\log u$. Therefore when u exceeds C_{44}, there exist at least $C_{45}(u/\log u)^2$ pairs of primes (p, q) with $u/2 < p < u$ and $u < q < 2u$ for which there exist integers $a\ (= a(p, q))$ and $b\ (= b(p, q))$ with $a \equiv A \pmod M$, $b \equiv B \pmod M$, $0 < |ca + db| \leq |c|Mu$, $0 < |ea + fb| \leq 2|cf - de|Mu$ and for which p divides $ca + db$ and q divides $ea + fb$. For each pair of primes (p, q) as above we put $t_{(p,q)} = F(a(p, q), b(p, q))$. We now take

$$u = x^{\frac{1}{r}}/(\max(|c|M, 2|cf - de|M)).$$

Plainly $|t_{(p,q)}|$ is at most x for all pairs (p, q) and provided that x exceeds C_{45} each integer $t_{(p,q)}$ contributes 1 to $S_k(x)$. Our result now follows.

8. Quadratic twists

In the next four sections we shall establish unconditional estimates for the number of twists of large rank of various elliptic curves. For many of our calculations in these sections we have employed the symbolic computation package MAPLE.

Our first result gives an unconditional analogue of the result of Gouvêa and Mazur [15] but with an exponent of $\frac{1}{7}$ in place of $\frac{1}{2}$. The proof depends on a construction used by Mestre [30] to prove that there are infinitely many elliptic curves over $\mathbb{Q}$ with given modular invariant and rank at least 2. Our contribution will be to make this result quantitative.

Theorem 3. *Let a and b be rational numbers and assume $ab(4a^3 + 27b^2) \neq 0$. There exist positive numbers C_{46} and C_{47}, which depend on a and b, such that if T is a real number larger than C_{46}, then the number of square-free integers d with $|d| \leq T$ for which the curve given by*

$$dy^2 = x^3 + ax + b$$

has rank at least 2 is at least $C_{47}T^{\frac{1}{7}}/(\log T)^2$.

Proof. Following Mestre we put

$$f(t) = t^3 + at + b, \qquad g(t) = (-\frac{b}{a})((t^4 + t^2 + 1)/(t^4 + t^2))$$

and

$$D(t) = a^4(t^2 + 1)^4t^6f(g(t)).$$

Let $P_1 = (g(t), (a^2(t^2+1)^2t^3)^{-1})$ and $P_2 = (t^2g(t), (a(t^2+1))^{-2})$ and note that P_1 and P_2 are points on E_D where E_D is given by the equation $D(t)y^2 = x^3 + ax + b$. Let E be the curve given by $y^2 = x^3 + ax + b$. The invariant differential ω_E on E is given by $\omega_E = \frac{dx}{2y}$. In the notation of Proposition 1, $\varphi_{P_1}^*\omega_E = ab(2t^2+1)\frac{dt}{s}$ and $\varphi_{P_2}^*\omega_E = -ab(t^5+2t^3)\frac{dt}{s}$ and so the rank of $E_D(\mathbb{Q}(t))$ is at least 2. The degree of D is 14 and D is divisible by t^2+1 in $\mathbb{Q}[t]$. Provided that $ab \neq 0$, $(t^2+1)^2$ does not divide D in $\mathbb{Q}[t]$. Put $F(X, Y) = Y^{14}D(X/Y)$. Let F_1 and F_2 be binary forms satisfying $F = F_1F_2^2$ with F_2 in $\mathbb{Z}[X, Y]$ and of maximal degree. Then $X^2 + Y^2$ divides F_1 and we may apply Lemma 1 and Theorem 2 to give our result.

Our next two theorems treat quadratic twists of special families of elliptic curves; for these families we are able to establish larger exponents than $\frac{1}{7}$.

Theorem 4. *Let a, b and c be rational numbers and put $A = -(a^2+ac+c^2)$. Assume that a and c are not both zero and that $4A^3 + 27b^2 \neq 0$. There exist positive numbers C_{48} and C_{49}, which depend on a, b and c, such that if T is a real number larger than C_{48}, then the number of square-free integers d with $|d| \leq T$ for which the curve given by*

$$dy^2 = x^3 + Ax + b$$

has rank at least 2 is at least $C_{49}T^{\frac{1}{4}}$.

Proof. Motivated by the construction of Schoof, §2 of [37] (see also [10], [29]), we put

$$r_1(t) = -ct^2 + 2at + a + c, \qquad r_2(t) = (a+c)t^2 + 2ct - a$$

and

$$D(t) = (r_1(t)^3 + Ar_1(t)(t^2+t+1)^2 + b(t^2+t+1)^3)(t^2+t+1).$$

We define $E_D/\mathbb{Q}(t)$ by the equation

$$D(t)y^2 = x^3 + Ax + b,$$

and put

$$P_i = \left(\frac{r_i(t)}{t^2+t+1}, \frac{1}{(t^2+t+1)^2}\right) \quad \text{for } i = 1, 2.$$

Here P_1 and P_2 are points from $E_D(\mathbb{Q}(t))$. The discriminant of D is $3^{13}A^{12}(4A^3+27b^2)^3$ and so, by assumption, is non-zero. Let $E/\mathbb{Q}$ be given by $y^2 = x^3 + Ax + b$. Let C be the curve given by $s^2 = D(t)$. Then, as in Proposition 1,

$$\varphi_{P_1}^*\omega_E = -\frac{1}{2}((2a+c)t^2 + 2(a+2c)t - a + c)\frac{dt}{s}$$

and

$$\varphi_{P_2}^*\omega_E = -\frac{1}{2}((-a+c)t^2 - 2(2a+c)t - a - 2c)\frac{dt}{s}.$$

Since a and c are not both zero the differentials are non-zero and linearly independent. Thus, by Proposition 1, the rank of $E_D(\mathbb{Q}(t))$ is at least 2. Our result now follows on appealing to Theorem 1 since the degree of D is at most 8 and the largest irreducible factor of D in $\mathbb{Q}[t]$ has degree at most 6.

Theorem 5. *Let a and b be rational numbers with $a(3a-b)(a+b) \neq 0$. There exist positive numbers C_{50} and C_{51}, which depend on a and b, such that if T is a real number larger than C_{50}, then the number of square-free integers d with $|d| \leq T$ for which the curve given by*

$$dy^2 = ax^3 + bx^2 + bx + a$$

has rank at least 2 is at least $C_{51} T^{\frac{1}{3}}$.

Proof. Let $D(t) = at^6 + bt^4 + bt^2 + a$ and denote by $E_D/\mathbb{Q}(t)$ the curve given by $D(t)y^2 = ax^3 + bx^2 + bx + a$. The points $(t^2, 1)$ and (t^{-2}, t^{-3}) from $E_D(\mathbb{Q}(t))$ are mapped by λ, as in Proposition 1, to the differentials $t\frac{dt}{s}$ and $-\frac{dt}{s}$ respectively, on the curve C given by $s^2 = D(t)$. The discriminant of D is $-64a^2(3a-b)^6(a+b)^2$ and our result now follows from Lemma 1 and Theorem 1.

The last example of quadratic twists presented here yields twists of rank at least 3 for a class of elliptic curves. It is based on an idea of Schoen [36] and in fact was discovered independently by him.

One starts with an elliptic curve E_a given by an equation

$$E_a: y^2 = x(x-1)(x-a).$$

We assume that both a and $a-1$ are squares in $\mathbb{Q}^*$. Under this assumption the curves E_a, $E_{1/a}$ and $E_{1/(1-a)}$ are isomorphic over $\mathbb{Q}$. Note that the condition is equivalent to a being of the form $(\frac{b^2+1}{2b})^2$ for $b \neq 0, \pm 1$ in $\mathbb{Q}$.

Using the projections $(x, y) \mapsto x: E \to \mathbb{P}^1$ one defines a fibre product

$$C = E_a \times_{\mathbb{P}^1} E_{1/a} \times_{\mathbb{P}^1} E_{1/(1-a)}.$$

Locally, C can be described by the equations

$$\begin{cases} y_1^2 = x(x-1)(x-a), \\ y_2^2 = x(x-1)\left(x - \frac{1}{a}\right), \\ y_3^2 = x(x-1)\left(x - \frac{1}{1-a}\right). \end{cases}$$

One can describe C alternatively using the functions x, y_1 and $u = \frac{y_1 y_2}{x(x-1)}$, $v = \frac{y_1 y_3}{x(x-1)}$. These satisfy the relations

$$\begin{cases} y_1^2 = x(x-1)(x-a), \\ u^2 = (x-a)\left(x - \frac{1}{a}\right), \\ v^2 = (x-a)\left(x - \frac{1}{1-a}\right). \end{cases}$$

It is easily checked that the latter two equations define a rational curve with a $\mathbb{Q}$-rational point. Parametrizing this curve allows us to prove our next result.

Theorem 6. *Let b be a rational number with $b \neq 0, 1, -1$. Put $a = (\frac{b^2+1}{2b})^2$. There exist positive numbers C_{52} and C_{53}, which depend on b, such that if T is a real number larger than C_{52}, then the number of square-free integers d with $|d| \leq T$ for which the curve given by*

$$dy^2 = x(x-1)(x-a)$$

has rank at least 3 is at least $C_{53}T^{\frac{1}{6}}$.

Proof. Put $A = a^3 - a^2 - a + 1$, $B = a^3 - a^2 + a$,

$$U = \frac{At^2 - B}{At^2 - 2At + B}, \quad V = \frac{At^2 - B}{-At^2 + 2Bt - B} \quad \text{and} \quad x(t) = \frac{U^2 - a^2}{a(U^2 - 1)}.$$

Next put

$$y(t) = (At^2 - B)/(8a^2(a-1)^2t^2(At^2 - (A+B)t + B)^2)$$

and

$$D(t) = y(t)^{-2}x(t)(x(t)-1)(x(t)-a).$$

Let $E/\mathbb{Q}$ be defined by $y^2 = x(x-1)(x-a)$ and $E_D/\mathbb{Q}(t)$ be defined by $D(t)y^2 = x(x-1)(x-a)$. Notice that $P_1 = (x(t), y(t))$, $P_2 = (ax(t), a^{\frac{3}{2}}y(t)/U)$ and $P_3 = (1 + (a-1)x(t), (a-1)^{\frac{3}{2}}y(t)/V)$ are in $E_D(\mathbb{Q}(t))$. In the notation of Proposition 1,

$$\varphi_{P_1}^*\omega_E = -a(a-1)(At^2 - 2Bt + B)(At^2 - 2At + B)\frac{dt}{s},$$

$$\varphi_{P_2}^*\omega_E = -a^{\frac{1}{2}}(a-1)(At^2 - 2Bt + B)(At^2 - B)\frac{dt}{s},$$

$$\varphi_{P_3}^*\omega_E = a(a-1)^{\frac{1}{2}}(At^2 - B)(At^2 - 2At + B)\frac{dt}{s},$$

and thus, since $A \neq B$, the rank of $E_D(\mathbb{Q}(t))$ is at least 3.

The discriminant of D is $2^{40}a^{70}(a-1)^{80}(a+1)^{20}(a^2-a+1)^{30}(2a-1)^{30}$ and the degree of D is 11. Further D factors as

$$-a(a-1)t(t-1)(At-B)(At^2 - (2a^3 - 6a^2 + 4a)t + B)$$
$$\cdot (At^2 - (A+B-1)t + B)((a-1)^3t^2 - 2(B-a^2)t + B)$$
$$\cdot ((A + 2a^2 - 2)t^2 - (2a^3 - 2a)t + B).$$

Thus we may apply Lemma 1 and, on clearing denominators in D, Theorem 1 to obtain our result.

9. Cubic twists

A cubic twist of an elliptic curve only exists if the elliptic curve admits an automorphism of degree 3. This means that such a curve has j-invariant 0, and it can be given by an equation $y^2 = x^3 + k$.

Here we will restrict ourselves to the curves studied by Zagier and Kramarz [47] and Mai [28], which are described by the equation

$$X^3 + Y^3 = m.$$

Define a morphism of degree 3 by

$$\xi = \frac{-XY}{m}, \qquad \eta = \frac{-Y^3}{m}.$$

The image is the curve given by

$$\eta^2 + \eta = m\xi^3,$$

or equivalently in homogeneous coordinates by $\eta\zeta(\eta+\zeta) = m\xi^3$ which one can dehomogenize alternatively as

$$xy(x+y) = m.$$

The morphism of degree 3 does not affect the rank. The curves we look at are the cubic twists of the curve $E/\mathbb{Q}$ given by $xy(x+y) = 1$. Note that Proposition 1 is applicable also for the curves given by our equation, since we can write it in the form $(8m\eta + 4m)^2 = (4m\xi)^3 + 16m^2$.

In a sense the most general parametrized twist E_t of E is given by the equation

$$xy(x+y) = t.$$

Since the curve defined by $s^3 = t$ is rational, it follows from Proposition 1 that $\operatorname{rank} E_t(\mathbb{Q}(t)) = 0$. A special case of a conjecture of Silverman (see p. 556 of [41]) then claims that for almost all specializations, the curve $xy(x+y) = N$ (and hence also $X^3 + Y^3 = N$) has rank at most 1. This contrasts with the experimental data found by Zagier and Kramarz [47].

The next thing we want is a polynomial $m(t)$ such that the curve C given by $s^3 = m(t)$ admits many morphisms to E with the property that the pullbacks of the standard invariant differential on E are all in the same eigenspace for the action of the automorphism of order 3. One way to try to find such $m(t)$ is to look for cases where the zeroes of $m(t)$ in $\mathbb{P}^1$ admit a lot of symmetry with respect to the action of $\mathrm{PGL}_2(\mathbb{Q})$. This will give automorphisms on the curve C and one can hope to find elliptic quotients to which the standard automorphism of degree 3 on C descends, which will force such a quotient to have j-invariant 0.

Such polynomials of degree 5 were studied by Igusa [21] who classified the genus 2 curves with additional automorphisms. One of them, suitably normalized for our purposes, is $m(t)$ where

$$m(t) = 2t(t-1)(t+1)(2t+1)(t+2).$$

Indeed our choice is motivated by some related work of Stewart [43] where the surface $xy(x+y) = m(t)$ is employed to prove that there are arbitrarily large integers h for which the Thue equation $xy(z+y) = h$ has at least 18 solutions in coprime integers x and y.

We now take C to be the curve given by $s^3 = m(t)$. This gives a model of a genus 4 curve; a basis of the holomorphic differentials which will be convenient for us is given by

$$\omega_1 = \frac{dt}{s}, \qquad \omega_2 = (1 + t + t^2)\frac{dt}{s^2},$$

$$\omega_3 = (1 - 2t - 2t^2)\frac{dt}{s^2}, \qquad \omega_4 = (2 + 2t - t^2)\frac{dt}{s^2}.$$

On C we define the involution

$$\sigma_1(t, s) = \left(\frac{1-t}{1+2t}, \frac{3s}{(1+2t)^2}\right).$$

One checks that the space of σ_1^*-invariant holomorphic differentials is generated by ω_3. Hence the quotient of C by σ_1 is elliptic; in fact invariant functions are

$$x = \frac{t(t-1)}{s} \quad \text{and} \quad y = \frac{-(t+2)(t+1)}{s}$$

which clearly satisfy the relation $xy(x+y) = 1$.

A second involution is given by

$$\sigma_2(t, s) = \left(\frac{t+2}{t-1}, \frac{3s}{(t-1)^2}\right).$$

Here ω_4 generates the space of invariant differentials. Invariant functions are given by

$$u = \frac{(2t+1)(t+1)}{s} \quad \text{and} \quad v = \frac{t-1}{s}$$

which also satisfy $uv(u+v) = 1$.

One can find another involution defined as

$$\sigma_3(t, s) = \left(-\frac{t+2}{2t+1}, \frac{-3s}{(2t+1)^2}\right).$$

This one has ω_2 as invariant differential and the functions

$$w = 2\frac{2t+1}{s} \quad \text{and} \quad z = 2\frac{t^2-1}{s}$$

are invariant. They satisfy $wz(w+z) = 4$. This equation defines an elliptic curve which has bad reduction at 2 while the curve given by $xy(x+y) = 1$ has good reduction at 2. Hence over $\mathbb{Q}$ the two elliptic curves are not isogenous.

Since this exhausts the biggest eigenspace for the action of the automorphism of degree 3, recall the proof of Corollary 1, we conclude that the $\mathbb{Q}(t)$-rank of the elliptic curve given by $xy(x+y) = m(t)$ is 2. From a geometric point of view it might be interesting to note the following result.

Proposition 2. *The smooth minimal surface associated with the equation*

$$xy(x+y) = 2t(t-1)(t+1)(2t+1)(t+2)$$

is an elliptic K3-surface with Picard number 20. *As an elliptic surface over the t-line it has rank* 6.

Proof. The fact that this defines a K3-surface is easily verified using the criterion given in [1], pp. 276–277. Using Tate's algorithm [44], pp. 46–52, one finds that this surface has six bad fibers. Each of these is of type IV which means that they look like three rational curves meeting transversally in one point.

The Shioda-Tate formula for the Picard number ρ then says that

$$\rho = r + 2 + 6 \cdot 2 = r + 14,$$

with r the $\mathbb{C}(t)$-rank of the elliptic curve defined by our equation. The discussion preceding this proposition implies that the $\mathbb{Q}(\sqrt[3]{4}, t)$-rank is at least 3. Hence using the action of the endomorphism ring on three such independent points one obtains a $\mathbb{Z}$-module of rank 6. It follows that $\rho \geq 6+14 = 20$. Since for all K3-surfaces the inequality $\rho \leq 20$ holds, this proves the proposition.

We will now discuss rank 3 twists of $X^3 + Y^3 = 1$. Write

$$m(t) = 2A(t)B(t)C(t)D(t)F(t)G(t)$$

with $A(t) = t$, $B(t) = 1$, $C(t) = t - 1$, $D(t) = t + 1$, $F(t) = t + 2$ and $G(t) = 2t + 1$. Our aim is to find for many t's a point (a, b) on $xy(x+y) = 2ABCDFG$ which is independent from the two points we already have.

Our basic idea is to try (a, b) such that $a + b = \lambda AB$. This choice of two of the six forms $A, \ldots, G$ may seem arbitrary, but in fact it is not. The points we had before also correspond to such pairs. Using isomorphisms of C one can change from one pair to another; on E this corresponds to such things as translation by a point of order 3 or the $[-1]$-map. In terms of such transformations, the pair (A, B) is the only one we have not yet discussed.

If a solution (a, b) satisfies $a + b = \lambda AB$, then obviously a, b are roots of the equation $X^2 - \lambda ABX + 2CDFG/\lambda = 0$. Hence the discriminant of this expression, or equivalently

$$\lambda^2 t^2 - \frac{16}{\lambda} t^4 - \frac{40}{\lambda} t^3 + \frac{40}{\lambda} t + \frac{16}{\lambda},$$

has to be a square. This is described by a family of elliptic curves over the λ-line; for example sections are given by $t = \pm 1$.

Originally we looked for fibers in this family which have infinitely many $\mathbb{Q}$-rational points. Then base changing the family given by $xy(x + y) = m(t)$ over the t-line to such an elliptic curve yields a family with three independent sections; the third one given by the point (a, b). Specializing to rational points on that elliptic curve then yields, in general, twists $xy(x+y) = m$ with rank at least 3. The main disadvantage of this method is that one obtains at best very weak density results on the number of twists obtained in this way. The point is that the number of rational points on an elliptic curve which have bounded height is much smaller than the number of such points on a rational curve.

One resolves this problem by taking instead of a base change to a fiber, a base change to a section of the family

$$Y^2 = \lambda^2 t^2 - \frac{16}{\lambda} t^4 - \frac{40}{\lambda} t^3 + \frac{40}{\lambda} t + \frac{16}{\lambda}.$$

Taking the point $(t = 1, Y = \lambda)$ as zero element for the group law, we computed that twice the point $(t = -1, Y = \lambda)$, which itself only leads to a degenerate 'twist' $X^3 + Y^3 = 0$, equals the point

$$\left(t = \frac{1-\lambda^3}{1+\lambda^3}, Y = \frac{\lambda(\lambda^6 - 17)}{(1+\lambda^3)^2}\right).$$

The base change of the family $xy(x+y) = m(t)$ to this section can be seen as a family over the λ-line, written as

$$xy(x+y) = m\left(\frac{1-\lambda^3}{1+\lambda^3}\right).$$

As an elliptic curve over $\mathbb{Q}(\lambda)$ this is isomorphic to

$$xy(x+y) = (1-\lambda^3)(1+\lambda^3)(3+\lambda^3)(3-\lambda^3).$$

On this model the point (a, b) which we have constructed can be written as

$$\left(4, \frac{\lambda^6 - 9}{2}\right).$$

To check that the three points we now have are indeed independent one studies the corresponding differentials. Our points yield morphisms from the curve given by $s^3 = (\lambda^6 - 1)(\lambda^6 - 9)$ to the elliptic curve given by $xy(x+y) = 1$. An invariant differential on this elliptic curve can be written as $\frac{dx}{x(2y+x)}$. The third point we constructed corresponds to the morphism

$$(\lambda, s) \mapsto \left(x = \frac{4}{s}, y = \frac{\lambda^6 - 9}{2s}\right).$$

From this description it is clear that the pull back of any differential on E is in the $+1$-eigenspace of the action on differentials of the automorphism given by $(\lambda, s) \mapsto (\zeta_6\lambda, s)$. The other two differentials are pullbacks under the morphism given by

$$(\lambda, s') \mapsto \left(t = \frac{1-\lambda^3}{1+\lambda^3}, s = \frac{-2\lambda s'}{(1+\lambda^3)^2}\right)$$

to the curve given by $s^3 = 2t(t-1)(t+1)(t+2)(2t+1)$. It follows easily that they are not in the $+1$-eigenspace of the automorphism mentioned.

Thus the elliptic curve defined over the function field $\mathbb{Q}(\lambda)$ by the equation

$$xy(x+y) = (\lambda^6 - 1)(\lambda^6 - 9)$$

has $\mathbb{Q}(\lambda)$-rank at least 3. We remark that we are able to prove that the $\mathbb{Q}(\lambda)$-rank is 3 and that the $\mathbb{C}(\lambda)$-rank is 14; we do not give the details here.

We shall now apply the above results to estimate the number of cubic twists of the elliptic curve given by $x^3 + y^3 = 1$ which have rank at least 2 or rank at least 3.

Theorem 7. *There exist positive numbers C_{54}, C_{55}, and C_{56} such that if T is a real number larger than C_{54}, then the number of cube-free integers d with $|d| \leq T$ for which the curve given by*

$$x^3 + y^3 = d$$

has rank at least 2 is at least $C_{55}T^{\frac{1}{3}}$, and for which it has rank at least 3 is at least $C_{56}T^{\frac{1}{6}}$.

Proof. This result follows from Lemma 1, our discussion above and Theorem 1. For the case of rank 2 we apply Theorem 1 to the binary form $F(X, Y) = 2XY(X-Y)(X+Y)(2X+Y)(X+2Y)$ whereas for the case of rank 3 we take $F(X, Y) = (X^6 - Y^6)(X^6 - 9Y^6)$.

10. Quartic twists

The only elliptic curves over $\mathbb{Q}$ for which quartic twists exist are those with j-invariant 1728. Such curves can be given by an equation $y^2 = x^3 + ax$.

Let $E/\mathbb{Q}$ be the elliptic curve given by the equation $y^2 = x^3 + x$. To get quartic twists of E of rank 2 we take $D(t) = -t^4 - 1$ and let $E_D/\mathbb{Q}(t)$ be given by the equation $y^2 = x^3 + D(t)x$. Notice that $P_1 = (-t^2, t)$ and $P_2 = (-1, t^2)$ are in $E_D(\mathbb{Q}(t))$. Further on taking C to be the Fermat curve $s^4 = -t^4 - 1$ and following the notation of Proposition 1 we find that $\varphi_{P_1}^* \omega_E = \frac{dt}{s^3}$ and $\varphi_{P_2}^* \omega_E = -t\frac{dt}{s^3}$. Thus the rank of $E_D(\mathbb{Q}(t))$ is at least 2.

Mestre [30] has shown how to find polynomials D for which the rank of $E_D(\mathbb{Q}(t))$ is at least 4. He proceeds as follows. Let x_1, x_2, x_3 be in $\mathbb{Q}(t)$. Put $x_4 = -(x_1+x_2+x_3)$, $p(x) = (x-x_1)(x-x_2)(x-x_3)(x-x_4) = x^4 + a_2x^2 + a_1x + a_0$ and $P_i = (x_i, x_i)$ for $i = 1, 2, 3, 4$. Plainly P_i is on the curve given by $x^4 + a_2y^2 + a_1y + a_0 = 0$ for $i = 1, 2, 3, 4$. Further, if $a_0 = -u^4$ with u in $\mathbb{Q}(t)$, then $(u, 0)$ is also on the curve. Note that if $X = -4a_2x^2$ and $Y = 4a_2x(2a_2y + a_1)$, then $Y^2 = X^3 + 4a_2(4a_2a_0 - a_1^2)X$.

Mestre [30] takes $u = 1$ and, appealing to a parametric solution due to Euler of $a_0 = -1$, he chooses

$$x_1 = t\left(\frac{2t^2 - 1}{2t^2 + 1}\right), \quad x_2 = \frac{(2t^2 - 1)}{2t(2t^2 + 1)} \quad \text{and} \quad x_3 = \frac{4t}{2t^2 - 1}.$$

Mestre then proves that the curve he gets when he specializes to $t = 1$ has rank at least 4 and so $E_{D_0}(\mathbb{Q}(t))$ has rank at least 4 where $D_0(t) = 4a_2(4a_2a_0 - a_1^2)$. Using the above ideas we shall prove our next result.

Theorem 8. *There exist positive numbers C_{57}, C_{58}, C_{59} and C_{60} such that if T is a real number larger than C_{57}, then the number of fourth power free integers d with $|d| \leq T$ for which the curve given by*

$$y^2 = x^3 + dx$$

has rank at least 2, 3 *or* 4 *is at least* $C_{58}T^{\frac{1}{2}}$, $C_{59}T^{\frac{1}{4}}$ *or* $C_{60}T^{\frac{1}{16}}/(\log T)^2$ *respectively.*

Proof. By the above discussion the rank of $E_D(\mathbb{Q}(t))$ is at least 2 when $D(t) = -t^4 - 1$. Applying Lemma 1 and Theorem 1 the result for the case of rank 2 follows.

Define $D_0(t)$ as above and put $D_1(t) = (2t(2t^2-1)(2t^2+1)^2)^4 D_0(t)$. Then

$$D_1(t) = (2t^2+3)(6t^2+1)(4t^4+12t^2+1)(12t^4+4t^2+3)$$
$$\cdot(64t^{12}+32t^{10}+304t^8+176t^6+76t^4+2t^2+1)(2t^2+1)^2(2t^2-1)^2.$$

Note that the rank of $E_{D_1}(\mathbb{Q}(t))$ is at least 4 since it equals the rank of $E_{D_0}(\mathbb{Q}(t))$ which is at least 4. Put $D_2(t) = D_1(t)/((2t^2+1)(2t^2-1))$. Since the degree of D_1 is 32 and the discriminant of D_2 is $-2^{854}3^{12}5^{16}83^4$ we may apply Lemma 1 and Theorem 2 to deduce our result for the case of rank 4.

If we choose $x_1 = 1$, $x_2 = t$ and $x_3 = t+2$ in Mestre's construction and put $D(t) = 16(t^2-3)(3t^2+8t+7)(t^2+t-1)(t^2+3t+3)$, then we deduce from Proposition 1 in the usual manner that the rank of $E_D(\mathbb{Q}(t))$ is at least 3 where E_D is given by $y^2 = x^3 + D(t)x$. Since the discriminant of D is $2^{76}3^65^6$ and the degree of D is 8 our result follows from Lemma 1 and Theorem 1.

11. Sextic twists

The only elliptic curves over $\mathbb{Q}$ for which sextic twists exist are those with j-invariant 0. Such curves can be given by an equation $y^2 = x^3 + k$.

Let $E/\mathbb{Q}$ be the elliptic curve given by the equation $y^2 = x^3 + 1$. We shall employ two different constructions to produce twists of E of large rank. The first construction produces twists of E of rank 3 and 4 while the second construction, due to Mestre [30], produces twists of rank 5 and 6.

We shall now describe our construction of rank 3 and rank 4 twists. Let x_1, x_2 and x_3 be in $\mathbb{Q}(t)$ and put $F(X, Y) = (X - x_1Y)(X - x_2Y)(X - x_3Y) + Y^3$. Put $P_i' = (x_i, 1)$ for $i = 1, 2, 3$ and $P_4' = (1, 0)$. Plainly P_1', P_2', P_3' and P_4' are points on the curve E_F given by $F(X, Y) = 1$. We shall choose x_1, x_2 and x_3 so that the rank of the $\mathbb{Q}(t)$-points of E_F is at least 3. If, in addition, $-x_1x_2x_3 + 1$ is a cube in $\mathbb{Q}(t)$, say v^3, then $P_5' = (0, \frac{1}{v})$ is another point on $F(X, Y) = 1$ and an appropriate choice of x_1, x_2 and x_3 will ensure that the rank of $E_F(\mathbb{Q}(t))$ is at least 4. Let $H(X, Y)$ be the quadratic covariant of F, let $G(X, Y)$ be the cubic covariant of F and let D_0 be the discriminant of F. We have

$$(4G)^2 = (4H)^3 - 27 \cdot 16 \cdot D_0 \cdot F^2 \tag{23}$$

(see Chapter 24 of [32]), and so there is a morphism defined over $\mathbb{Q}(t)$ from E_F to the curve E_D given by $y^2 = x^3 + D$ where $D = -27 \cdot 16 \cdot D_0$. Thus we obtain a family of sextic twists of E.

Our initial construction of families of rank 5 and rank 6 twists of E depended on work of Craig [8], [9]. In [8] Craig proved that infinitely many

imaginary quadratic fields have a subgroup of the class group isomorphic to the direct product of three copies of the cyclic group of order 3. To do so he constructed a polynomial D of degree 24 (see §4 of [8]) and exhibited five different points in $E_D(\mathbb{Q}(t))$. Using Proposition 1 one may check that the rank of $E_D(\mathbb{Q}(t))$ is at least 5. Since the discriminant of D is $-2^{184}3^{300}7^{18}647^3$ we may apply Theorem 2 to deduce that rank 5 twists of E occur with exponent $\frac{1}{12}$. In [9] Craig sharpened his earlier result by proving that there are infinitely many imaginary quadratic fields for which the 3-rank of the ideal class group is at least 4. Nakano [33] deduced from Craig's construction that there are infinitely many twists of E of rank 6. Using the polynomial D of §8 of [9] and proceeding in the usual manner one finds that rank 6 twists of E occur with exponent $\frac{1}{72}$.

We are able to obtain larger exponents however, by employing the following construction of Mestre [30]. Let $x_1, \ldots, x_5$ be in $\mathbb{Q}(t)$. Put

$$\begin{aligned} x_6 &= -(x_1 + \cdots + x_5), \\ p(X) &= (X - x_1)\cdots(X - x_6) \\ &= X^6 + a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0, \\ g(X) &= X^2 + a_4/3 \end{aligned}$$

and

$$r(X) = r_3X^3 + r_2X^2 + r_1X + r_0,$$

where $r_3 = a_3$, $r_2 = a_2 - a_4^2/3$, $r_1 = a_1$ and $r_0 = a_0 - (a_4/3)^3$. Next put

$$F(X, Y) = r_3X^3 + r_2X^2Y + r_1XY^2 + r_0Y^3,$$

let E_F denote the curve $F(X, Y) = -1$ and put $P_i' = (\frac{x_i}{g(x_i)}, \frac{1}{g(x_i)})$ for $i = 1, \ldots, 6$. We shall choose $x_1, \ldots, x_5$ so that $E_F(\mathbb{Q}(t))$ has rank at least 5. Further if r_3 is a cube in $\mathbb{Q}(t)$, say v^3, then $P_7' = (-\frac{1}{v}, 0)$ is in $E_F(\mathbb{Q}(t))$. Mestre takes

$$\begin{aligned} x_1 = -x_2 &= 126(35t - 19)(14t - 13)(t + 1), \\ x_3 &= 63(-980t^3 + 3549t^2 - 3084t + 1135), \\ x_4 &= 63(1127t^3 - 3108t^2 + 3525t - 988), \\ x_5 &= -113876t^3 + 265629t^2 - 259980t + 69103 \end{aligned}$$

and

$$x_6 = 104615t^3 - 293412t^2 + 232197t - 78364.$$

In this case $r_3 = (2x_1/3)^3$ and by specializing to $t = 1$ he proves that the rank of $E_F(\mathbb{Q}(t))$ is at least 6. We now use (23) as before to obtain sextic twists of E.

Theorem 9. *There exist positive numbers C_{61}, C_{62}, C_{63}, C_{64} and C_{65} such that if T is a real number larger than C_{61}, then the number of sixth power free integers d with $|d| \leq T$ for which the curve given by*

$$y^2 = x^3 + d$$

has rank at least 3, 4, 5 or 6 is at least $C_{62}T^{\frac{1}{3}}$, $C_{63}T^{\frac{1}{6}}$, $C_{64}T^{\frac{1}{9}}/(\log T)^2$ or $C_{65}T^{\frac{1}{27}}/(\log T)^2$ respectively.

Proof. We shall prove the result for rank 3 and 4 twists with the first construction we discussed above. Accordingly take $x_1 = 1$, $x_2 = t$, $x_3 = 2t + 1$. Then using (23) and Proposition 1 we find that the rank of $E_D(\mathbb{Q}(t))$ is at least 3 where E_D is given by $y^2 = x^3 + D(t)$ and

$$D(t) = 2^4 3^3(-4t^6 + 8t^4 - 40t^2 + 31).$$

Our result now follows from Lemma 1 and Theorem 1 on noting that the discriminant of D is $2^{56}3^{30}5^6 7^6 31$.

For rank 4 twists we take $x_1 = (1-t^2)/2$, $x_2 = 2(t^2+t+1)$ and $x_3 = t^2-t+1$. Then, using (23) and Proposition 1 we find that the rank of $E_D(\mathbb{Q}(t))$ is at least 4 where E_D is given by $y^2 = x^3 + D(t)$ and

$$\begin{aligned} D(t) = &-6075t^{12} - 38070t^{11} - 81513t^{10} - 83106t^9 - 67797t^8 - 39528t^7 \\ &- 27270t^6 - 58968t^5 - 89181t^4 - 84834t^3 - 52353t^3 - 23814t + 9261. \end{aligned}$$

As before, our result follows from Lemma 1 and Theorem 1 on noting that the discriminant of D is $2^{64}3^{72}5^6 7^{18}13^3 31^3 43^3 73^3 241^3 13807861$.

For rank 5 twists we take $x_1 = 1$, $x_2 = 2$, $x_3 = -3$, $x_4 = 0$, $x_5 = t$ and $x_6 = -t$ in Mestre's construction. Again by (23) and Proposition 1 we find that the rank of $E_D(\mathbb{Q}(t))$ is at least 5 where E_D is given by $y^2 = x^3 + D(t)$ and

$$D(t) = \frac{-64}{27}(t^{18} + 2973t^{12} - 369249t^6 + 11764900).$$

Our result now follows from Lemma 1 and Theorem 2 on noting that the discriminant of D is $-2^{232}3^{30}5^{28}7^{48}11^{18}$.

Finally with the choice of $x_1, \ldots, x_6$ made by Mestre above and the transformation (23) we obtain $D(t)$ for which the rank of $E_D(\mathbb{Q}(t))$ is at least 6. The degree of D is 54 and the discriminant

$$2^{2756}3^{8838}5^{18}7^{2886}13^{24}17^6 19^{18}23^3 31^{16}47^6 \cdots$$

is non-zero. Our result follows from Lemma 1 and Theorem 2.

12. Parity

In this section we briefly recall a conjecture on the parity of the rank of the Mordell-Weil group of an elliptic curve. We shall restrict our attention to the case of twists of a given curve.

Let $E/\mathbb{Q}$ be an elliptic curve with conductor N. Suppose that E is given by the equation $y^2 = f(x)$. Let d be a square-free non-zero integer and E_d be given by the equation $dy^2 = f(x)$. Let $r(d)$ denote the rank of $E_d(\mathbb{Q})$.

Parity conjecture for quadratic twists. *Suppose that* d *and* $2N$ *are coprime. Then*

$$(-1)^{r(d)-r(1)} = \chi_d(-N),$$

where χ_d *is the quadratic Dirichlet character belonging to the field* $\mathbb{Q}(\sqrt{d})$.

We refer to §2 of [5] for a discussion of this conjecture; see [22], [23] for some recent work on this problem. We also have corresponding conjectures for cubic, quartic and sextic twists. Birch and Stephens [2] worked out explicit versions of these conjectures in the cubic and quartic cases. Recently Liverance [25] has done this for the sextic case.

Parity conjecture for cubic twists. *Let* d *be a cube free integer and let* E_d *be the elliptic curve given by* $x^3+y^3=d$. *Let* $r(d)$ *denote the rank of* $E_d(\mathbb{Q})$. *We have*

$$(-1)^{r(d)} = -w_3 \cdot \prod_{p\neq 3} w_p,$$

where

$$w_3 = \begin{cases} -1 & \text{if } d \equiv \pm 1, \pm 3 \pmod 9, \\ 1 & \text{otherwise}, \end{cases}$$

and

$$w_p = \begin{cases} -1 & \text{if } p|d \text{ and } p \equiv 2 \pmod 3, \\ 1 & \text{otherwise.} \end{cases}$$

Parity conjecture for quartic twists. *Let* d *be a fourth power free integer and suppose* $d \not\equiv 0 \pmod 4$. *Let* E_d *be the curve given by* $y^2 = x^3 + dx$ *and let* $r(d)$ *denote the rank of* $E_d(Q)$. *Then*

$$(-1)^{r(d)} = \frac{d}{|d|} \cdot w_2 \cdot \prod_{p\neq 2} w_p,$$

where

$$w_2 = \begin{cases} -1 & \text{if } d \equiv 1, 3, 11, 13 \pmod{16}, \\ 1 & \text{otherwise}, \end{cases}$$

and

$$w_p = \begin{cases} -1 & \text{if } p^2 \| d \text{ and } p \equiv 3 \pmod 4, \\ 1 & \text{otherwise.} \end{cases}$$

Note that the condition $d \not\equiv 0 \pmod 4$ above is not significant since $r(d) = r(-4d)$. This follows from the fact that the curves E_d and E_{-4d} are 2-isogenous over $\mathbb{Q}$.

Parity conjecture for sextic twists. *Let* d *be a sixth power free integer with* d *factoring as* $d = 2^u 3^v d_6$ *where* $(d_6, 6) = 1$. *Let* E_d *be the curve given by* $y^2 = x^3 + d$ *and let* $r(d)$ *denote the rank of* $E_d(\mathbb{Q})$. *Then*

$$(-1)^{r(d)} = -w_2 w_3 \prod_{p\neq 2,3} w_p,$$

where

$$w_2 = \begin{cases} -1 & \text{if } 2 \nmid u \text{ or } 2|u,\ d_2 \equiv 1 \pmod 4,\ u \neq 4, \\ +1 & \text{if } 2|u,\ d_2 \equiv -1 \pmod 4 \text{ or } u = 4,\ d_2 \equiv 1 \pmod 4, \end{cases}$$

$$w_3 = \begin{cases} -1 & \text{if } v \equiv -1 \pmod 3 \text{ or } 3|v,\ d_3 \equiv \pm 2 \pmod 9, \\ +1 & \text{if } v \equiv +1 \pmod 3 \text{ or } 3|v,\ d_3 \equiv \pm 4 \pmod 9, \\ (-1)^v\left(\frac{d_3}{3}\right) & \text{if } 3|v,\ d_3 \equiv \pm 1 \pmod 9, \end{cases}$$

$$w_p = \begin{cases} -1 & \text{if } p|d,\ p \equiv 2 \pmod 3, \\ +1 & \text{otherwise}, \end{cases}$$

and where d_n *is the largest divisor of* d *prime to* n *(with the same sign as* d*), so that* $d_2 = 3^v d_6$ *and* $d_3 = 2^u d_6$.

In many instances it is possible to employ the above conjectures to conclude that, for reasons of parity, the rank of a twist of a given elliptic curve is larger by one than our constructions indicate. This is the approach taken by Gouvêa and Mazur [15]. Let $E/\mathbb{Q}$ be given by the equation $y^2 = x^3 + Ax + B$. They observe that if $D(t) = t^3 + At + B$, then certainly the point $(t, 1)$ is in $E_D(\mathbb{Q}(t))$ where E_D is given by $D(t)y^2 = x^3 + Ax + B$. Let C be the conductor of E and observe that we may assume that A and B are integers divisible by M where $M = 12 \cdot C$ by changing the model for E. By the parity conjecture for quadratic twists and the law of quadratic reciprocity there is a set U, consisting of half of the coprime residue classes modulo M, with the property that if d is positive and belongs to a member of U, then the rank of E_d is even. Put $F(X, Y) = Y(X^3 + AXY^2 + BY^3)$ and $F_1(X, Y) = F(X + jMY, Y)$ where j is the smallest positive integer for which $F_1(X, 1)$ has non-positive roots. Since $F_1(X, Y) \equiv YX^3 \pmod M$ there are integers a_0 and b_0 for which $F_1(a_0, b_0)$ belongs to a member of U. Thus, as noted by Gouvêa and Mazur, whenever $d = F_1(a, b)$ is sufficiently large, with $a \equiv a_0 \pmod M$ and $b \equiv b_0 \pmod M$, the rank of E_d is at least 1 and so, by the parity conjecture, is even and at least 2. In our proof of Theorem 1 we estimate $R_k(x)$ by considering terms $F(a, b)$ where a and b are positive integers. Since $F_1(a, b)$ is positive when a and b are positive, we may appeal to Theorem 1 to obtain a slight refinement of their result; the exponent of $\frac{1}{2} - \varepsilon$ in their lower bound may be replaced by $\frac{1}{2}$.

Similarly we may recover the result of Mai on cubic twists of E where $E/\mathbb{Q}$ is given by the equation $X^3 + Y^3 = 1$. Let $D(t) = t^3 + 1$ and observe that $(t, 1)$ is a point in $E_D(\mathbb{Q}(t))$ where E_D is given by $X^3 + Y^3 = D(t)$. On recalling the discussion at the start of §9 and applying Proposition 1 we see that the rank of $E_D(\mathbb{Q}(t))$ is at least 1. Put $F(X, Y) = X^3 + Y^3$ and note that if $X \equiv 1 \pmod 9$ and $Y \equiv 0 \pmod 9$, then $X^3 + Y^3 \equiv 1 \pmod 9$. If d is a square-free positive integer with $d \equiv 1 \pmod 9$, then the number of primes congruent to 2 modulo 3 which divide d is even. Thus, by the parity conjecture for cubic twists, the rank of $X^3 + Y^3 = d$ is even.

Observe that $F(a, b)$ is positive when a and b are positive. Thus, by Theorem 1, there are positive numbers C_{66} and C_{67} such that the number of square-free positive integers t with $t \leq x$ for which there are integers a and

b with $a \equiv 1 \pmod 9$, $b \equiv 0 \pmod 9$ and $a^3 + b^3 = t$ is at least $C_{66}x^{2/3}$ for x at least C_{67}. Therefore, by Lemma 1 and the parity conjecture for cubic twists, there are positive numbers C_{68} and C_{69} such that the number of positive integers d with $d \leq x$ for which the rank of $X^3 + Y^3 = d$ is even and at least 2 is at least $C_{68}x^{2/3}$ for x greater than C_{69}.

As a final application let $F(X, Y) = (X^6 - Y^6)(X^6 - 9Y^6)$ and observe that if a and b are positive integers with $a < b$, then $F(a, b)$ is positive. It follows, as in the proof of Lemma 2, that the number of pairs of integers (a, b) with $1 \leq a \leq x$, $1 \leq b \leq x$, $a < b$, $a \equiv 1 \pmod 9$ and $b \equiv 0 \pmod 9$ for which $F(a, b)$ is square-free is $\frac{1}{2}C_{13}x^2 + O(x^2/(\log x)^{\frac{1}{3}})$; the estimates for the error terms in the proof are unchanged. Similarly, on modifying the proof of Theorem 1 by replacing U by the set of pairs of integers (a, b) in U with $a < b$ and using the above observation we deduce that there are positive numbers C_{70} and C_{71} such that if x exceeds C_{70}, then the number of square-free positive integers t with $t \leq x$ and $t \equiv 1 \pmod 9$ for which there exist integers a and b with $F(a, b) = t$ is at least $C_{71}x^{\frac{1}{6}}$. Thus by Lemma 1, Proposition 3 and the parity conjecture for cubic twists there exist positive numbers C_{72} and C_{73} such that the number of positive integers d with $d \leq x$ for which the rank of $X^3 + Y^3 = d$ is even and at least 4 is at least $C_{72}x^{\frac{1}{6}}$ for x greater than C_{73}.

REFERENCES

1. F. Beukers and J. Stienstra, *On the Picard-Fuchs equation and the formal Brauer group of certain elliptic K3-surfaces*, Math. Ann. **271** (1985), 269–304.
2. B. J. Birch and N. Stephens, *The parity of the rank of the Mordell-Weil group*, Topology **5** (1966), 295–299.
3. B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves.* I, J. Reine Angew. Math. **212** (1963), 7–25.
4. ———, *Notes on elliptic curves.* II, J. Reine Angew. Math. **218** (1965), 79–108.
5. ———, *Elliptic curves and modular functions*, Modular Functions of One Variable IV (B. J. Birch and W. Kuyk, eds.), Lecture Notes in Math., vol. 476, Springer-Verlag, Berlin, New York, and Heidelberg, 1975, pp. 2–32.
6. A. Brumer, *The average rank of elliptic curves.* I, Invent. Math. **109** (1992), 445–472.
7. A. Brumer and O. McGuinness, *The behaviour of the Mordell-Weil group of elliptic curves*, Bull. Amer. Math. Soc. (N.S.) **23** (1990), 375–382.
8. M. Craig, *A type of class group for imaginary quadratic fields*, Acta Arith. **22** (1973), 449–459.
9. ———, *A construction for irregular discriminants*, Osaka J. Math. **14** (1977), 365–402.
10. D. S. Dummit, *Néron models, Tate curves and Mestre's technique of using elliptic curves to construct quadratic fields with non-trivial 5-rank*, Number Theory Seminar, Montréal, 1989.
11. P. Erdős and K. Mahler, *On the number of integers which can be represented by a binary form*, J. London Math. Soc. **13** (1938), 134–139.
12. G. Frey, *On the Selmer group of twists of elliptic curves with $\mathbb{Q}$-rational torsion points*, Canad. J. Math. **40** (1988), 649–665.
13. M. Fried, *Constructions arising from Néron's high rank curves*, Trans. Amer. Math. Soc. **281** (1984), 615–631.

14. D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Number Theory (Proc. Conf. in Carbondale, 1979) (M. B. Nathanson, ed.), Lecture Notes in Math., vol. 751, Springer-Verlag, Berlin, New York, and Heidelberg, 1979, pp. 108–118.
15. F. Gouvêa and B. Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc. **4** (1991), 1–23.
16. G. Greaves, *Power-free values of binary forms*, Quart. J. Math. Oxford Ser. (2) **43** (1992), 45–65.
17. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th ed., Oxford Univ. Press, London and New York, 1979.
18. T. Honda, *Isogenies, rational points and section points of group varieties*, Japan. J. Math. **30** (1960), 84–101.
19. C. Hooley, *On power-free values of polynomials*, Mathematika **14** (1967), 21–26.
20. ———, *Applications of sieve methods to the theory of numbers*, Cambridge Univ. Press, Cambridge, 1976.
21. J. I. Igusa, *Arithmetic variety of moduli for genus two*, Ann. of Math. (2) **72** (1960), 612–649.
22. K. Kramer, *Arithmetic of elliptic curves upon quadratic extension*, Trans. Amer. Math. Soc. **264** (1981), 121–135.
23. K. Kramer and J. Tunnell, *Elliptic curves and local ε-factors*, Compositio Math. **46** (1982), 307–352.
24. J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, Algebraic Number Fields (A. Fröhlich, ed.), Academic Press, London and New York, 1977, pp. 409–464.
25. E. Liverance, *Heights of Heegner points in a family of elliptic curves*, Ph.D. Thesis, University of Maryland, 1992.
26. K. Mahler, *Zur Approximation algebrischer Zahlen.* I (*Über den gröszten Primteiler binärer Formen*), Math. Ann. **107** (1933), 691–730.
27. ———, *Zur Approximation algebrischer Zahlen.* III (*Über die mittlere Anzahl der Darstellungen groszer Zahlen durch binäre Formen*), Acta Math. **62** (1933), 91–166.
28. L. Mai, *The analytic rank of a family of elliptic curves*, Canad. J. Math. **45** (1993), 847–862.
29. J.-F. Mestre, *Courbes elliptiques et groupes de classes d'idéaux de certains corps quadratiques*, J. Reine Angew. Math. **343** (1983), 23–35.
30. ———, *Rang des courbes elliptiques d'invariant donné*, C. R. Acad. Sci. Paris Sér. I **314** (1992), 919–922.
31. ———, *Courbes elliptiques de rang* ≥ 12 *sur* $\mathbb{Q}(t)$, C. R. Acad. Sci. Paris Sér. I **313** (1991), 171–174.
32. L. J. Mordell, *Diophantine equations*, Academic Press, London and New York, 1969.
33. S. Nakano, *Construction of pure cubic fields with large 2-class groups*, Osaka J. Math. **25** (1988), 161–170.
34. A. Néron, *Propriétés arithmetiques de certaines familles de courbes algebriques*, Proc. Internat. Congr. (Amsterdam, 1954), vol. III, Noordhoff, Groningen, and North-Holland, Amsterdam, 1956, pp. 481–488.
35. U. Schneiders and H. G. Zimmer, *The rank of elliptic curves upon quadratic extension*, Computational Number Theory (A. Pethö, M. Pohst, H. C. Williams, and H. G. Zimmer, eds.), Walter de Gruyter, Berlin and New York, 1991, pp. 239–260.
36. C. Schoen, *Bounds for rational points on twists of constant hyperelliptic curves*, J. Reine Angew. Math. **411** (1990), 196–204.
37. R. J. Schoof, *Class groups of complex quadratic fields*, Math. Comp. **41** (1983), 295–302.
38. J.-P. Serre, *Lectures on the Mordell-Weil theorem*, Vieweg, Braunschweig/Wiesbaden, 1989.
39. T. Shioda, *An infinite family of elliptic curves over* $\mathbb{Q}$ *with large rank via Néron's method*, Invent. Math. **106** (1991), 109–119.

40. J. H. Silverman, *Heights and the specialization map for families of abelian varieties*, J. Reine Angew. Math. **342** (1983), 197–211.
41. ———, *Divisibility of the specialization map for families of elliptic curves*, Amer. J. Math. **107** (1985), 555–565.
42. ———, *The arithmetic of elliptic curves*, Graduate Texts in Math., vol. 106, Springer-Verlag, Berlin, New York, and Heidelberg, 1985.
43. C. L. Stewart, *On the number of solutions of polynomial congruences and Thue equations*, J. Amer. Math. Soc. **4** (1991), 793–835.
44. J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular Functions of One Variable. IV (B. J. Birch and W. Kuyk, eds.), Lecture Notes in Math., vol. 476, Springer-Verlag, New York and Heidelberg, 1975, pp. 33–52.
45. J. T. Tate and I. R. Shafarevich, *The rank of elliptic curves*, Soviet Math. Dokl. **8** (1967), 917–920.
46. J. Top, *Néron's proof of the existence of elliptic curves over* $\mathbb{Q}$ *with rank at least* 11, R. U. Utrecht Dept. of Math. preprint series, no. 476, 1987.
47. D. Zagier and G. Kramarz, *Numerical investigations related to the L-series of certain elliptic curves*, J. Indian Math. Soc. **52** (1987), 51–69.

DEPARTMENT OF PURE MATHEMATICS, THE UNIVERSITY OF WATERLOO, WATERLOO, ONTARIO, CANADA N2L 3G1
E-mail address: cstewart@watserv1.uwaterloo.ca

VAKGROEP WISKUNDE, UNIVERSITY OF GRONINGEN, P.O. BOX 800, 9700 AV GRONINGEN, THE NETHERLANDS
E-mail address: top@math.rug.nul